CAUSE NO. 035723

NATIONAL OILWELL VARCO, LP	§	IN THE DISTRICT COURT OF
	§	
Plaintiff	§	
	§	
v.	§	
	§	GRIMES COUNTY, TEXAS
JULIO C. GARZA and	§	
ARRAY TECHNOLOGIES, INC.	§	
	§	12th
Defendant	§	____ JUDICIAL DISTRICT COURT

ORDER GRANTING PLAINTIFFS' EMERGENCY MOTION FOR EXPEDITED COMPUTER FORENSIC IMAGING & ANALYSIS

After hearing the arguments of counsel and considering Plaintiff's Emergency Motion for Expedited Computer Forensic Imaging & Analysis, the Court finds that National Oilwell Varco, LP ("NOV") has shown good cause for the requested expedited computer forensic imaging and analysis. The Motion is granted.

Therefore, the Court orders that expedited computer forensic imaging and analysis will be allowed as follows only to the extent that the discovery is relevant to the Original Petition and Application for a Temporary Restraining Order and Temporary Injunction or reasonably calculated to lead to the discovery of admissible evidence in the Original Petition and Application:

1. ***Capture Phase***

a. "Subject Electronic Devices" includes:

i. Electronic storage devices and accounts (e.g. tablets, smartphones, hard drives, thumb drives, recordable optical disks, Cloud email and Cloud storage accounts, such as Dropbox, Google Docs, etc.), in Julio Garza's possession, custody, or control that have been connected to his employment with NOV, his NOV email account or any other electronic storage device owned by NOV.

ii. All personal computers (PCs), laptops, smart phones, tablets, or other electronic storage devices (e.g. hard drives, thumb drives, recordable optical disks, Cloud email and Cloud storage accounts, such as Dropbox, Google Docs, etc.), in Julio Garza's possession, custody, or control that have been connected to his employment with NOV.

EXHIBIT
B

iii. All computers (PCs), laptops, smart phones, tablets, or other electronic storage devices (e.g. hard drives, thumb drives, recordable optical disks, Cloud email and Cloud storage accounts, such as Dropbox, Google Docs, etc.), in Array Technologies, Inc.'s possession, custody, or control to which Julio Garza has had access or which have been connected to electronic storage devises or email accounts to which or from which Julio Garza sent or received emails including but not limited to emails with NOV information.

iv. Other personal computers (PCs), laptops, smart phones, tablets, or other electronic storage devices (e.g. hard drives, thumb drives, recordable optical disks, Cloud email and Cloud storage accounts, such as Dropbox, Google Docs, etc.), that the Court later rules there is good cause for production after an expedited hearing on the issue.

b. No more than three business days after the Court enters this Order, and before any files containing NOV information have been accessed, modified, or deleted, Defendants will give all Subject Electronic Devices to CyberEvidence, Inc. ("CyberEvidence") or its affiliate or otherwise provide CyberEvidence with access to such Subject Electronic Devices. Defendants will simultaneously provide CyberEvidence with any necessary user names, logins, or passwords necessary to access any of the Subject Electronic Devices.

c. CyberEvidence will create bit-by-bit forensic images of the entire contents found on the Subject Electronic Devices. CyberEvidence will conduct the forensic imaging as expeditiously as reasonably possible and promptly return the devices to Defendants when it is complete.

d. After the forensic imaging, CyberEvidence will maintain all information in its sole possession, except as provided below. The forensic images themselves will not leave CyberEvidence's possession or be shared with Plaintiff or its counsel.

e. Within five business days after the imaging, the expert will provide both parties with a report describing the Subject Electronic Devices Defendants produced and the actions CyberEvidence took with respect to forensically imaging each device. The report will include a detailed description of the device inspected, including the name of the manufacturer and model and serial number of the equipment wherever possible.

2. *Analysis Phase*

a. CyberEvidence will recover all reasonably accessible data and documents from the forensic images of the Subject Electronic Devices as directed by Plaintiffs' counsel, including, without limitation, all word-processing documents, e-mail messages, PowerPoint or similar presentations, spreadsheets, and other files, including deleted files. CyberEvidence will then search the recovered data.

b. CyberEvidence will use search terms provided by NOV to search the forensic images of the Subject Electronic Devices specifically to find NOV's information including, but not limited to, NOV's information regarding its drilling motor and friction reducing products, services or technologies.

c. CyberEvidence will provide an inventory list of all documents that return as positive hits based on the search term list directly to the parties' respective counsel. The inventory list will contain the name and corresponding file system metadata fields for each file and folder.

d. CyberEvidence will next provide all documents that return as positive hits based on the search term list directly to Defendants' counsel. Defendants' counsel will review the documents, and within three business days after receiving the documents, Defendants' counsel will provide Plaintiffs' counsel and CyberEvidence with a list of documents that Defendants' believe are: (i) "Privileged" because the document is protected by the attorney-client privilege or attorney work product doctrine, (ii) "Private" because the document contains solely Defendants' own personal, private information (including, without limitation, personal health or financial information) and is not relevant to the subject matter of the pending action and is unrelated to the claim or defense of any party, or (iii) "Confidential" or "Attorneys' Eyes Only" in accordance with the proposed Protective Order (or any protective order ultimately entered). CyberEvidence will then give Plaintiff forensically sound copies of all positive hit documents not designated "Privileged" or "Private." Documents designated "Privileged" or "Private" will be withheld from production at this time. Documents designated "Confidential" or "Attorneys' Eyes Only" will be afforded the protections set out in any protective order ultimately entered.

e. If Plaintiffs question the "Privileged" or "Private" designation of any document, they may notify Defendants in writing of the disputed document. The Parties will then attempt to resolve the designation dispute among themselves. For example, the Parties may agree that: (i) a disputed document may be produced to Plaintiffs' counsel designated as Attorney's Eyes Only under the proposed Protective Order (or any protective order ultimately entered); (ii) Plaintiffs' counsel may be provided with a copy of the disputed document that has been redacted to exclude the material that drew the designation; or (iii) CyberEvidence may be permitted to review the disputed document and confirm its proper designation to Plaintiffs. If the parties cannot resolve a designation dispute, an expedited motion to compel may be filed. Any response to the motion must be filed within three business days.

f. To determine whether any deleted data should be recovered as a document, CyberEvidence may send Defendants' counsel a list of the textual context of the part of a partially recovered document in which a positive hit was made based on the search terms above. Defendants' counsel will have one business day from the date CyberEvidence provides the list of textual context to designate any document or text as: (i) "Privileged" because the information is protected by the attorney-client privilege or attorney work product doctrine, or (ii) "Private" because the information is purely Defendants' own personal, private information (including, without limitation, personal health or financial information) and is not relevant to the subject matter of the pending action and is unrelated to the claim or defense of any party. CyberEvidence will then provide the list of any textual context not designated as Privileged or Private to Plaintiffs' counsel so Plaintiffs' counsel can determine if that positive hit document warrants the expense of further forensic recovery. The list of textual context will be automatically designated as Attorneys' Eyes Only as that term is defined in the proposed Protective Order (or any protective order ultimately entered).

g. In addition to searching the forensic images as described above, CyberEvidence may – at Plaintiffs' request – conduct additional standard forensic analyses on the forensic images to determine whether any of NOV's information has been deleted, copied, or disseminated to any other devices, including searching for possible vectors of data theft. If CyberEvidence performs such analyses, it will inform Plaintiffs of its findings.

3. ***Destruction Phase***

a. Once a final judgment in this suit has been rendered and the appellate deadlines have expired, CyberEvidence will destroy all forensic images that are in the company's custody, after receiving written authorization from both parties' counsel.

b. CyberEvidence and the parties' respective counsel will then destroy any materials generated using the forensic images in accordance with any protective order ultimately entered.

4. ***Costs***

a. All expenses incurred by CyberEvidence for the tasks outlined above will be borne by Plaintiffs.

b. This provision for payment to CyberEvidence is not to be construed as an indication that such expenses are or are not recoverable costs in this or any other suit.

Signed on 6/3/2022, 2022.

Judge Presiding